

## § 2001.42

(a) Protecting it from persons without authorized access to that information, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person;

(b) Meeting safeguarding requirements prescribed by the agency head; and

(c) Ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

## § 2001.42 Standards for security equipment.

(a) *Storage.* The Administrator of the General Services Administration (GSA) shall, in coordination with agency heads originating classified information, establish and publish uniform standards, specifications, qualified product lists or databases, and supply schedules for security equipment designed to provide secure storage for classified information. Whenever new secure storage equipment is procured, it shall be in conformance with the standards and specifications established by the Administrator of the GSA, and shall, to the maximum extent possible, be of the type available through the Federal Supply System.

(b) *Destruction.* Effective January 1, 2011, only equipment listed on an Evaluated Products List (EPL) issued by the National Security Agency (NSA) may be utilized to destroy classified information using any method covered by an EPL. However, equipment approved for use prior to January 1, 2011, and not found on an EPL, may be utilized for the destruction of classified information until December 31, 2016. Unless NSA determines otherwise, whenever an EPL is revised, equipment removed from an EPL may be utilized for the destruction of classified information up to six years from the date of its removal from an EPL. In all cases, if any such previously approved equipment needs to be replaced or otherwise requires a rebuild or replacement of a critical assembly, the unit must be taken out of service for the destruction in accordance with this section. The Administrator of the GSA shall, to the

## 32 CFR Ch. XX (7–1–12 Edition)

maximum extent possible, coordinate supply schedules and otherwise seek to make equipment on an EPL available through the Federal Supply System.

## § 2001.43 Storage.

(a) *General.* Classified information shall be stored only under conditions designed to deter and detect unauthorized access to the information. Storage at overseas locations shall be at U.S. Government-controlled facilities unless otherwise stipulated in treaties or international agreements. Overseas storage standards for facilities under a Chief of Mission are promulgated under the authority of the Overseas Security Policy Board.

(b) *Requirements for physical protection*—(1) *Top Secret.* Top Secret information shall be stored in a GSA-approved security container, a vault built to Federal Standard (FED STD) 832, or an open storage area constructed in accordance with § 2001.53. In addition, supplemental controls are required as follows:

(i) For GSA-approved containers, one of the following supplemental controls:

(A) Inspection of the container every two hours by an employee cleared at least to the Secret level;

(B) An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation. Acceptability of Intrusion Detection Equipment (IDE): All IDE must be in accordance with standards approved by ISOO. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the agency head; or

(C) Security-In-Depth coverage of the area in which the container is located, provided the container is equipped with a lock meeting Federal Specification FF-L-2740.

(ii) For open storage areas covered by Security-In-Depth, an IDS with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(iii) For open storage areas not covered by Security-In-Depth, personnel responding to the alarm shall arrive within five minutes of the alarm annunciation.